0360

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Julian DURAND

Serial No.: 09/893,589

Filed: June 29, 2001

For: SYSTEM FOR PROTECTING COPYRIGHTED MATERIALS

PRELIMINARY AMENDMENT

Assistant Commissioner of Patents
Washington, D.C. 20231

September 21, 2001

Sir:

In connection with the above-identified application please enter the following preliminary amendments.

IN THE SPECIFICATION:

Please replace the paragraph beginning at page 4, line 19, with the following rewritten paragraph:

Thus, in operation, the user uses wireless device 14 to contact server 12. An authentication method is performed using known mechanisms such as Shared Secrets. Once both parties are sure of the identity of the other, the terminal may request data to be sent. This data may be the next page in an electronic book when the user presses a next page button or may be a request for the next 30 seconds of a song or video that is running on the terminal. This may be manual requests as in the case of an eBook, or automatic requests in the case of streaming. The server receives the request and records situation information such as the time of request (and perhaps location if the device is location aware) and passes the request onto the digital rights management engine. This engine them compares the request with its stored knowledge of the users right to access the copyrighted material. If the user has sufficient rights, authorization is

provided to the server. When the server receives authorization, it is recorded in the audit trail storage device. This storage may not be modified. The information as stored therein is used to make charges where appropriate to the user. At the same time, the data is formatted and delivered to the wireless device for use.

Please replace the paragraph beginning at page 5, line 14 with the following rewritten paragraph:

Figure 3 is a flowchart showing the steps involved in the first embodiment. In step 100, the wireless device and the server mutually authenticate the identity of each other. Mutual authentication is desirable but not a necessity. At a minimum, the client must be authenticated to determine if it has rights to access content. It is desirable for the client to also authenticate the server to ensure that the correct server is providing the information. For example, it would be good for a consumer to know that the weather warning came from the government rather than a hacker trying to get her out of the house. In step 102, a request is given by the user and received by the server. It is then passed on to the digital rights management engine. In step 104, the authorization is rendered by the digital rights management engine to the server. The authorization is stored in the audit trail storage device in step 106. The content is then rendered by the server in step 108.

Please replace the paragraph beginning at page 5, line 20, with the following rewritten paragraph:

Figure 4 is a flowchart showing the steps of the method used in the embodiment of Figure 2. Steps 100 to 106 operate in the same fashion as similarly numbered steps in Figure 3. However, the final step of rendering the information 108 has been replaced by two steps 110 and 112. In step 110 the content is first rendered and stored in storage device 22. In the final step, instructions are then provided to forward as

necessary data from the storage device 22. In fact, this is more of the high bandwidth case of sending pre-rendered data straight to the screen or audio of a super light weight device. In the case where there is an always-on connection, which is not very fast, simple control information and content formatting information is sent.

Please replace the paragraph beginning at page 5, line 25, with the following rewritten paragraph:

Figure 5 shows another arrangement of the system and its functional connections. The protected data base 18 stores the immediate keys, the unique ID numbers and the rights expression. This information is fed to the server device 30 and an audit trail 20 is generated which records events. The device 30 is connected to the decryption engine 24 in a wireless device. A mutually authenticated secure channel is generated using some type of wireless connection such as Blue Tooth, IRDA, GRPS or other wireless connections. Storage device 28 stores encrypted data objects which are sent to the decryption engine. Data which has been decrypted is then sent to the rendering application 26 along the secure channel for the decrypted data content.

Please replace the paragraph beginning at page 6, line 8, with the following rewritten paragraph:

Figure 6 is a diagram which shows files in the content storage device and how the data is arranged. That is, for each song or other copyrighted data which is stored, the file includes information about the title, artist, album, length, tempo, user, metadata and the song or other copyrighted information which is encrypted with the media key. A unique identifier is also stored to identify a particular content object.

Please replace the paragraph beginning at page 6, line 12, with the following rewritten paragraph:

Figure 7 shows the filing arrangement of data in the digital rights management engine 18. Thus for each user, a file is kept which is a database of all content owned by the user. Each record identifies a particular piece of content with, at a minimum, a unique identifier, a media key and rights expression relating to the unique ID of the content.

Please replace the paragraph beginning at page 6, line 17, with the following rewritten paragraph:

Figure 9 is a diagram showing the storage of the event ID in a file. The event ID is part of the Event Record, which is part of the audit trail that is written. The Event Record data elements should be configurable at implementation, but at a minimum, it should record: unique ID for the record (Event ID); date & time (from a trusted clock); content requested / accessed (Content – ID); action requested (view, listen, forward, copy); success of request (many denied requests are suspicious and should be reported as anomalies to the system): target device; end time. Event records may be used where the user is charged a price per unit of time. This is quite similar to the existing Call Detail records (CDRs) in the GSM world. At the end of the month a procedure would tally outstanding amounts. These event records may be used to audit the usage and access to content for the purposes of reporting anomalies or cracks in the system.

Please replace the paragraph beginning at page 7, line 10, with the following rewritten paragraph:

The present system is especially useful when wireless networks are very widespread. Such networks may be of any speed depending on the complexity of the terminal. A lower speed network would require components such as trusted storage and trusted rendering applications. A higher bandwidth environment will allow the

terminal to be very simple and "thin", requiring little more than a display, an authentication mechanism, battery and appropriate communications circuitry.

Please replace the paragraph beginning at page 7, line 15, with the following rewritten paragraph:

In both Figures 1 and 2, server 12 would normally be different from the server which controls the wireless network. However, it is possible that it would sit in the same box if appropriate for the arrangement of the network. It should also be remembered that this type of system could be used in a wired network with the same advantages, except that the requirements to have a small, lightweight and portable device are not so important. In particular, with the addition of device profiling, it enables any user of the network (fixed or wireless) to log into their rights server and access their content on any other device irrespective of differences in physical size and other attributes.

REMARKS

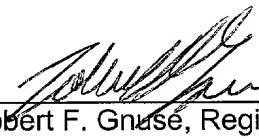
Entry of the above changes is respectfully requested.

Attached hereto is a marked-up version of the changes made to the claims by the present amendment.

To the extent necessary, please charge any shortage in the fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 01-2135 (017.38953X00).

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP



Robert F. Gnuse, Registration No.27,295

RFG:dmw
(703) 312-6600 – phone
(703) 312-6666 – fax
rgnuse@antonelli.com - e-mail

VERSION WITH MARKINGS TO SHOW CHANGES MADE

Thus, in operation, the user uses wireless device 14 to contact server 12. An authentication method is performed using known mechanisms such as [the Diffie-Helmann Exchange of] Shared Secrets. Once both parties are sure of the identity of the other, the terminal may request data to be sent. This data may be the next page in an electronic book when the user presses a next page button or may be a request for the next 30 seconds of a song or video that is running on the terminal. This may be manual requests as in the case of an eBook, or automatic requests in the case of streaming. The server receives the request and records situation information such as the time of request (and perhaps location if the device is location aware) and passes the request onto the digital rights management engine. This engine them compares the request with its stored knowledge of the users right to access the copyrighted material. If the user has sufficient rights, authorization is provided to the server. When the server receives authorization, it is recorded in the audit trail storage device. This storage may not be modified. The information as stored therein is used to make charges where appropriate to the user. At the same time, the data is formatted and delivered to the wireless device for use.

Please replace the paragraph beginning at page 5, line 14 with the following rewritten paragraph:

Figure 3 is a flowchart showing the steps involved in the first embodiment. In step 100, the wireless device and the server mutually authenticate the identity of each other. Mutual authentication is desirable but not a necessity. At a minimum, the client must be authenticated to determine if it has rights to access content. It is desirable for

the client to also authenticate the server to ensure that the correct server is providing the information. For example, it would be good for a consumer to know that the weather warning came from the government rather than a hacker trying to get her out of the house. In step 102, a request is given by the user and received by the server. It is then passed on to the digital rights management engine. In step 104, the authorization is rendered by the digital rights management engine to the server. The authorization is stored in the audit trail storage device in step 106. The content is then rendered by the server in step 108.

Please replace the paragraph beginning at page 5, line 20, with the following rewritten paragraph:

Figure 4 is a flowchart showing the steps of the method used in the embodiment of Figure 2. Steps 100 to 106 operate in the same fashion as similarly numbered steps in Figure 3. However, the final step of rendering the information 108 has been replaced by two steps 110 and 112. In step 110 the content is first rendered and stored in storage device 22. In the final step, instructions are then provided to forward as necessary data from the storage device 22. In fact, this is more of the high bandwidth case of sending pre-rendered data straight to the screen or audio of a super light weight device. In the case where there is an always-on connection, which is not very fast, simple control information and content formatting information is sent.

Please replace the paragraph beginning at page 5, line 25, with the following rewritten paragraph:

Figure 5 shows another arrangement of the system and its functional connections. The protected data base 18 stores the immediate keys, the unique ID numbers and the rights expression. This information is fed to the server device 30 and an audit trail 20 is generated which records events. The device 30 is connected to the decryption engine 24 in a wireless device. A mutually authenticated secure channel is generated using some type of wireless connection such as Blue Tooth, IRDA, GRPS or other wireless connections. Storage device 28 stores encrypted data objects which are sent to the decryption engine. Data which has been decrypted is then sent to the rendering application 26 along the secure channel for the decrypted data content.

Please replace the paragraph beginning at page 6, line 8, with the following rewritten paragraph:

Figure 6 is a diagram which shows files in the content storage device and how the data is arranged. That is, for each song or other copyrighted data which is stored, the file includes information about the title, artist, album, length, tempo, user, metadata and the song or other copyrighted information which is encrypted with the media key. A unique identifier is also stored to identify a particular content object.

Please replace the paragraph beginning at page 6, line 12, with the following rewritten paragraph:

Figure 7 shows the filing arrangement of data in the digital rights management engine 18. Thus for each user, a file is kept which [has] is a database of all content owned by the user. Each record identifies a particular piece of content with, at a

minimum, a unique identifier, a media key and rights expression relating to the unique ID of the content. [The file also establishes rights vouchers for that person.]

Please replace the paragraph beginning at page 6, line 17, with the following rewritten paragraph:

Figure 9 is a diagram showing the storage of the event ID in a file. The event ID is part of the Event Record, which is part of the audit trail that is written. The Event Record data elements should be configurable at implementation, but at a minimum, it should record: unique ID for the record (Event ID); date & time (from a trusted clock); content requested / accessed (Content – ID); action requested (view, listen, forward, copy); success of request (many denied requests are suspicious and should be reported as anomalies to the system); target device; end time. Event records may be used where the user is charged a price per unit of time. This is quite similar to the existing Call Detail records (CDRs) in the GSM world. At the end of the month a procedure would tally outstanding amounts. These event records may be used to audit the usage and access to content for the purposes of reporting anomalies or cracks in the system.

Please replace the paragraph beginning at page 7, line 10, with the following rewritten paragraph:

The present system is especially useful when wireless networks are very widespread. Such networks may be of any speed depending on the complexity of the terminal. A lower speed network would require components such as trusted storage and trusted rendering applications. A higher bandwidth environment will allow the

terminal to be very simple and "thin", requiring little more than a display, an authentication mechanism, battery and appropriate communications circuitry.

Please replace the paragraph beginning at page 7, line 15, with the following rewritten paragraph:

In both Figures 1 and 2, server 12 would normally be different from the server which controls the wireless network. However, it is possible that it would sit in the same box if appropriate for the arrangement of the network. It should also be remembered that this type of system could be used in a wired network [although the advantages gained thereby are not as important as in a wireless network] with the same advantages, except that the requirements to have a small, lightweight and portable device are not so important. In particular, with the addition of device profiling, it enables any user of the network (fixed or wireless) to log into their rights server and access their content on any other device irrespective of differences in physical size and other attributes.